(12) UK Patent Application (19) GB (11) 2 273 629 (13) A

(43) Date of A Publication 22.06.1994

(21) Application No 9324898.7

(22) Date of Filing 03.12.1993

(30) Priority Data
(31) 992278 (32) 16.12.1992 (33) US

(71) Applicant(s)
American Telephone and Telegraph Company

(Incorporated in USA - New York)

32 Avenue of the Americas, New York,
N Y 10013-2412, United States of America

(72) Inventor(s)
Charles Arthur Witschorik

(74) Agent and/or Address for Service
K G Johnston
AT&T (UK) Ltd, 5 Mornington Road,
WOODFORD GREEN, Essex, IG8 0TU,
United Kingdom

(51) INT CL[5]
H04M 3/42 , G07F 7/12 , H04M 11/00

(52) UK CL (Edition M)
H4K KFD KFH

(56) Documents Cited
EP 0501697 A2 WO 86/07480 A1

(58) Field of Search
UK CL (Edition M) H4K KFD KFH KOC KOD3
INT CL[5] G07F , H04M
Online databases: WPI

(54) Method for visual authentication by images transmitted over a telecommunication system

(57) A merchant transmits over a channel in a telecommunications system the credit card number of a person seeking to making a credit card purchase. The request is received by a database and utilized to locate a record corresponding to the credit card number. A visual image stored in the database which corresponds to the credit card number is transmitted to a visual display terminal at the merchant location to assist the merchant in authentication of the authority of the person presenting the credit card.

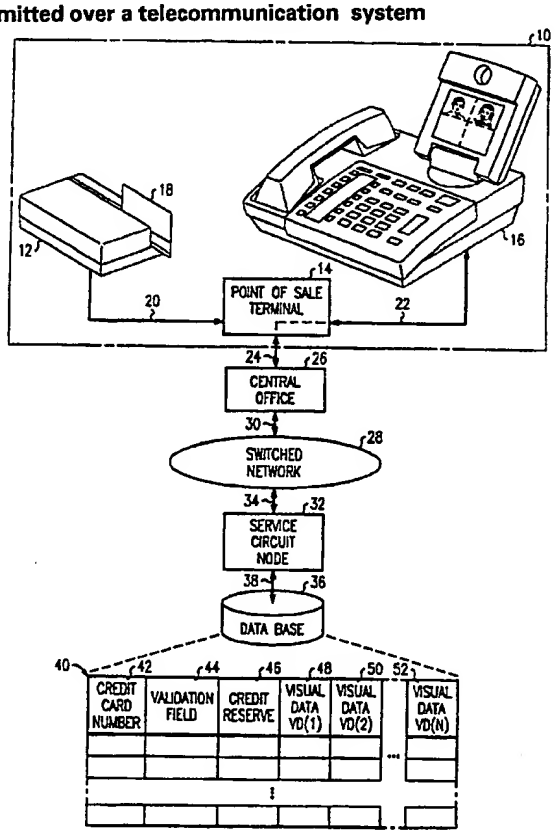

FIG. 1

GB 2 273 629 A

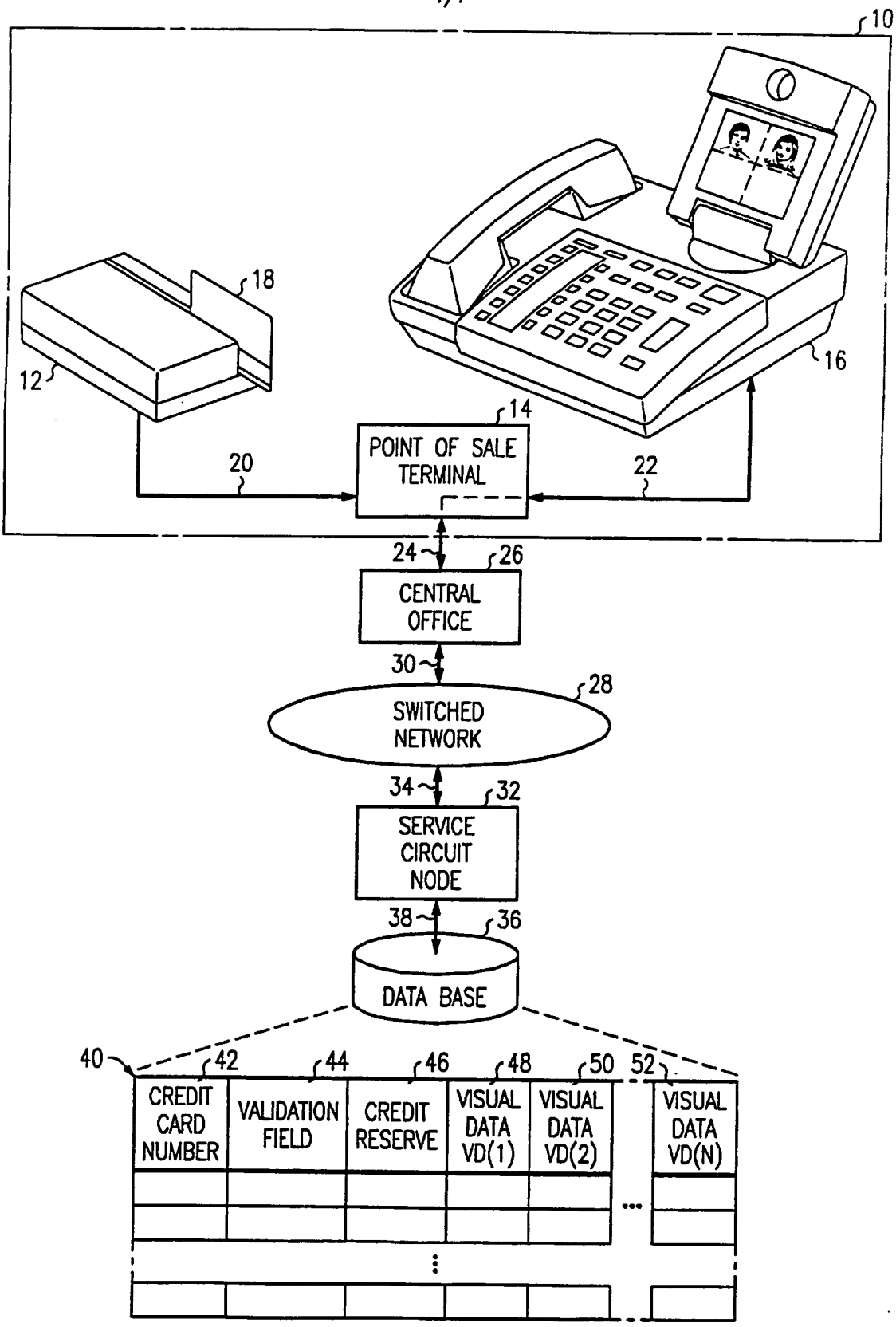
10
18
12
16
14
POINT OF SALE TERMINAL
20
22
24
26
CENTRAL OFFICE
30
28
SWITCHED NETWORK
34
32
SERVICE CIRCUIT NODE
38
36
DATA BASE
40
42
44
46
48
50
52
CREDIT CARD NUMBER
VALIDATION FIELD
CREDIT RESERVE
VISUAL DATA VD(1)
VISUAL DATA VD(2)
VISUAL DATA VD(N)

FIG. 1

METHOD FOR VISUAL AUTHENTICATION BY IMAGES TRANSMITTED OVER A TELECOMMUNICATION SYSTEM

Background of the Invention

This invention is generally directed to the process of verifying a person's identity or authority for a particular purpose. This invention is particularly, but not exclusively, suited for use in permitting a merchant to visually authenticate if a person requesting to charge a purchase to a credit card is authorized to utilize the corresponding credit card account.

Various types of encryption keys and secret passwords have been utilized to authenticate the authority of a person to obtain access to restricted information or locations. Encrypted messages may be transmitted over the public switched telephone network to a receiving party having a decrypting key allowing the receiving party to recover a corresponding plain text message. The use of encryption keys for authentication purposes require relatively sophisticated communication devices and system control in order to remain effective.

Authentication that a person is authorized to enter into a financial transaction in a business setting normally relies upon conventional practices. For example, a merchant desiring to authenticate a person's authority to make a credit card purchase may compare a signature on the back of a credit card to the signature of the person requesting such a purchase. Personal identification can be made by comparing a photograph disposed on a credit card or other identification such as a driver's license to the person seeking to make a credit card purchase. It is also known to utilize a personal identification number (PIN) as a password which may be required to be entered or given for a requested transaction to be processed, such as when utilizing an automatic teller machine.

The use of photographs for authentication is desirable for normal business use. However, enclosing photographs in a credit card is relatively expensive for the company issuing the credit card. The problem becomes even more difficult when a primary credit card applicant desires to have other persons authorized to utilize the same card. It is possible for a person seeking to defraud a merchant to tamper with a credit card or other identification so as to replace an existing photograph with the photograph of the person seeking to commit the fraud. Thus, there exists a need for an improved method by which visual authentication can be made of persons seeking to gain access to restricted rights or accounts.

Summary of the Invention

It is an object of the present invention to provide an improved authentication method wherein an inquirer is automatically provided a visual image of the authorized user(s) associated with an identification data word such as a credit card number.

In accordance with an embodiment of the present invention, a merchant utilizes a point-of-sale terminal to transmit a credit card number via a communication channel to an authorization database. The database contains the validation status of each credit card number or account and a corresponding field(s) of pictures of authorized users of each credit card number. Upon processing a request for credit card validation and determining the credit card number to be valid, the database transmits the digitally stored picture(s) to a visual display terminal of the merchant preferably in combination with a confirmation number indicating authorization to charge the account, thereby enabling the merchant to make a visual comparison to authenticate the authority of the person presenting the credit card.

Brief Description of the Drawing

FIG. 1 illustrates a pictorial representation of a telecommunications system, which in accordance with the present invention, can be utilized to provide visual authentication.

Detailed Description

FIG. 1 illustrates a system which incorporates an embodiment of the present invention. In the exemplary embodiment, a merchant or inquirer at location 10 has access to a credit card reader 12, a point-of-sale terminal 14 and a visual display terminal 16 which may comprise an AT&T VideoPhone. The magnetic card reader 12 reads the account number typically embedded on a magnetic strip on the card as credit card 18 is passed through the reader. The account number is transmitted by reader 12 over data channel 20 to point-of-sale terminal 14. The video display terminal 16 is coupled by communication channel 22 with communication link 24 indirectly through point-of-sale terminal 14.

Communication channel 24 couples the point-of-sale terminal 14 and video display terminal 16 to a telephone central office 26. The central office 26 which may comprise an AT&T 5ESS® switch, is connected to a switched network 28 by communication channel 30. The switch network 28 may comprise part of the public switched telephone network or a private communications network. A service circuit node 32 such as available from AT&T is coupled to switch network 28 by communication channel 34. The service circuit node 32 comprises a

computer controlled peripheral to a switching network and is utilized to provide auxiliary services. A database 36 is coupled to the service circuit node 32 by communication channel 38. The database 36 in accordance with the preferred embodiment of the present invention comprises an independent computer controlled database in which data is stored in a nonvolatile storage memory such a computer disk drive.

In the illustrative embodiment, database 36 stores data in a format as shown in table 40 in which data is stored in different fields for each credit card number or account. The table consists of a matrix in which different credit card numbers are stored in column 42. Each row of the table contains information related to the corresponding credit card number. Column 44 is a validation field utilized to determine if the corresponding credit card number is valid. Column 46 contains the remaining credit reserve of the credit card account. Columns 44, 50, and 52 contain visual data VD1, VD2, and VD(N), respectively, which represent visual information for each credit card number. The visual data comprises digitized images such as pictures of authorized users which may be stored in a compressed data format in the table in order to conserve storage space. In the preferred embodiment of the present invention, it is contemplated that a picture of each authorized user will be stored in the visual data fields. However, other visual information such as images of the signature of authorized users or fingerprints of authorized users could be utilized. As used herein, visual information means a pictorial representation of a feature or attribute of a person which can aid in identifying the person. It will be apparent that the information contained in table 40 must be collected for each credit card number in database 36 in order to be utilized for validation purposes discussed below. It will also be apparent that table 40 will need to be updated in order to maintain current and accurate data relating to each credit card number or account.

In accordance with an exemplary method of the present invention, visual information is provided by the telecommunications system to help a merchant or inquirer validate that the person requesting to make a credit card purchase is authorized. Although this example focuses on credit card usage and authentication of persons authorized, it will be apparent that the method in accordance with the present invention can be utilized to validate or authenticate persons requiring access to various benefits or locations in addition to the illustrative example.

Upon a customer's request for a credit card purchase, the merchant transmits an identification data word such as the credit card number via a telecommunications system to a database having credit card validation capability.

Typically, the merchant may utilize the credit card reader 12 to automatically read the credit card number from credit card 18 by passing the credit card through the reader. The credit card number is transmitted to a point-of-sale terminal 14 located at the merchant location 10. The point-of-sale terminal utilizing conventional modem technology transmits the request for validation including credit card number by channel 24 to a destination having validation capabilities. In the illustrative example the request is processed and passes through central office 26, switched network 28, and service circuit node 32 before reaching validation database 36.

Upon receiving the request for validation, database 36 initiates a search of column 42 of the data contained in table 40 to identify if a corresponding card number exists. If such a number is located, the validation data field 44 for the corresponding card is checked to determine if the card is valid. As an additional step the database may check the credit reserve data in column 46 to determine if sufficient credit remains for the requested purchase where the amount of the purchase has been transmitted along with the credit card number. The database 36 also identifies corresponding visual data consisting of digitized pictures of authorized users which may be utilized to authenticate the authority of the credit card presenter.

Assuming that a corresponding card number was located by database 36 and determined to be valid, database 36 transmits a confirmation number authorizing the purchase through the same return path upon which the request was received. The point-of-sale terminal 14 accepts the received confirmation number as account authorization. Database 36 preferably also utilizes the same path to transmit corresponding visual data related to the credit card number as stored in table 40 to video display terminal 16. The video display terminal receives the visual data and displays the corresponding image or images upon its visual display screen at the merchant location 10. Preferably, the image is frozen on the screen either by the video display terminal or by the database repetitively sending the same visual data. The merchant can then make a visual comparison to determine if the person requesting the credit card purchase is an authorized user by comparing the presented picture of authorized person(s) to the person requesting credit card authorization. If the merchant determines that the credit card user matches a displayed picture, the merchant would then accept the requested credit card purchase with substantial assurance that the person utilizing the credit card is an authorized user.

Database 36 may either comprise part of the telecommunications system or may be maintained as a private database utilized by different issuers of credit cards. If a plurality of databases are utilized for different credit card issuers, the above example would proceed the same with the only difference being that the request would be routed to the appropriate database by the telecommunications system. In the illustrative embodiment the same database was utilized to perform the traditional credit card account/number validation utilizing columns 44 and 46, and to store the related visual data. However, a database that stores traditional account validation data may contain identification of individual authorized users such as by social security number or personal identification number which can be utilized as addresses for a separate database containing visual data corresponding to each user.

It will be apparent to those skilled in the art that the functions performed by the equipment utilized at the merchant location 10 may be performed by a single piece of equipment based on a personal computer in which communications over channel 24 are provided by a conventional modem and the visual data received from the database converted into pixel information displayed upon a connected monitor.

In accordance with the present invention a merchant or other inquirer having responsibility to validate a person's requested access to certain benefits or locations is provided with an improved means for making the authorization judgement. Visual images such as pictures provide a substantially higher degree of reliability for making the authorization determination than other means based upon indicia present upon the card presented by the requesting person. It is known that cards can be modified to change the intended validation indicia such as by substituting a different signature or inserting a different photograph than was originally present on the card. In accordance with the present invention the received image is outside of the control of a person who wrongfully acquires and attempts to utilize a credit card. Thus, the present invention provides a substantially improved authentication technique which should deter the stealing and attempted use of stolen credit cards because of the higher risk associated with wrongful attempted use.

Although an embodiment of the present invention has been illustrated and described herein, the scope of the invention is defined by the claims which follow.

Claims:

1. In a public switched telecommunications network (PSTN) having a computer controlled peripheral that facilitates auxiliary telecommunication services, the PSTN coupled to a plurality of point of sale merchants that process credit card transactions with customers, the merchants having means for transmitting a customer's credit card number and visual display equipment coupled to the PSTN, a method for providing authentication to a merchant of a customer's identity prior to acceptance by the merchant of a credit card transaction, the method comprising the steps of:

receiving at said computer controlled peripheral a customer's credit card number sent by a requesting merchant using said transmitting means;

said computer controlled peripheral using the received credit card number to locate a corresponding record in a database associated with the peripheral, said record including a stored visual image associated with the corresponding customer;

said computer controlled peripheral transmitting said visual image to the visual display equipment of the requesting merchant, whereby the merchant is given visual identification information to use in authentication of the customer.

2. The method according to claim 1 further comprising the step of determining if said credit card number is valid by checking validation data stored in a corresponding record stored in the database associated with said computer controlled peripheral.

3. The method according to claim 2 wherein said validation determining step comprises the step of using a validation field in the same record in which said visual image is stored for the same credit card number.

4. The method according to claim 2 further comprising the step of sending data from said computer controlled peripheral to the requesting merchant indicative of whether said credit card number is valid, said validity indicative data being sent automatically when said visual image is sent.

5. The method according to claim 1 further comprising the step of routing a transmission of a customer's credit card number from a requesting merchant to said computer controlled peripheral which is part of said PSTN so that processing is handled solely within said PSTN.

6. The method according to claim 1 wherein said visual image comprises a picture of one person authorized to use the associated credit card.

7. The method according to claim 6 wherein said visual image comprises a picture of each person authorized to use the associated credit card.

Patents Act 1977 Examiner's report to the Comptroller under Section 17 (The Search report)	Application number GB 9324898.7
Relevant Technical Fields (i) UK Cl (Ed.M) H4K: KFD; KFH; KOC; KOD3 (ii) Int Cl (Ed.5) GO7F, HO4M	Search Examiner Al STRAYTON Date of completion of Search 8 MARCH 1994
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE: WPI	Documents considered relevant following a search in respect of Claims :- ALL

Categories of documents

X:	Document indicating lack of novelty or of inventive step.	P:	Document published on or after the declared priority date but before the filing date of the present application.
Y:	Document indicating lack of inventive step if combined with one or more other documents of the same category.	E:	Patent document published on or after, but with priority date earlier than, the filing date of the present application.
A:	Document indicating technological background and/or state of the art.	&:	Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
A	EPO 501 697 A2	(AT8T)	
X	WO 86/07480 A1	(MEDIA NET) See page 12 line 24 to page 13 line 11	1 and 6 at least

Databases:The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).